UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/692,261	10/23/2003	Jon Cargille	MS1-1781US	1559

22801 7590 08/04/2008

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
TRUVAN, LEYNNA THANH	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
08/04/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/692,261	CARGILLE ET AL.	
	Examiner	Art Unit	
	Leynna T. Truvan	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 May 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4-7,12-15,19,21,26-29 and 31-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *2,8-11,20,22-25 and 30* is/are allowed.

6)☒ Claim(s) *1,4-7,12-15,19,21,26-29 and 31-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *9/4/07 & 1/15/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1, 3-7, 12-19, 21, 26-29, and 31-33 are pending.

Claims 2, 8-11, 20, 22-25, and 30 are cancelled by applicant.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on *5/16/2008* has been entered.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on *9/4/2008* was filed after the mailing date of the *Non-Final Rejection on 4/2/2007*. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

4. The information disclosure statement (IDS) submitted on *1/15/2008* was filed after the mailing date of the *Final Rejection on 11/16/2007*. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Response to Arguments

5. Applicant's arguments with respect to claims have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 3-7, 12-19, 21, 26-29, and 31-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Harman, et al. (US 6,807,636) in view of Benantar, et al. (US 5,765,153).

As per claim 1:

Harman disclose a kernel-level transaction system, comprising:

a memory; (col.11, lines 4-13 and col.12, lines 48-50)

one or more processors operatively coupled to the memory and disposed within one or more devices; (col.12, lines 32-60)

a transaction manager disposed within each device, each said transaction manager including a plurality of kernel objects (col.14, lines 20-32 and col.15, lines 18-35; *modules being called or loaded by the kernel are given as kernel objects*) to implement a transaction having plural operations (col.14, lines 13-17 and col.18, lines 20-33), wherein the plurality of kernel objects include a transaction object to represent a transaction (col.14, lines 42-50 and 58-67 and col.15,

lines 36-40; *transaction module is given as security request and/or monitor associated with the application or service module*), a resource manager object to represent a resource participating in the transaction (col.14, lines 30-42 and 51-52 and col.15, lines 55-67; *a resource object given as component, i.e. interface, controller, device server (col.17, lines 33-52)*), and *[an enlistment object to plural kernel objects to enlist participants in the transaction]*, wherein the transaction is performed at the kernel levels; and (col.14, lines 24-28 and col.17, lines 1-3)

a security descriptor, applied to at least one of the kernel objects, to identify at least one user (col.13, lines 1-26), to identify one of the operations of the transaction that may be performed on the kernel object to which the security descriptor is applied (col.18, line 59 – col.19, line 11), and to identify a right indicating that the identified user is permitted or prohibited to perform the operation. (col.20, lines 29-63)

Although, Harman includes transaction object to represent a transaction which is a service module/application to plural kernel objects but does not go into details of an enlistment object to enlist participants.

Benantar's invention improves security in objected oriented system where the security system is a point of control for the security information and allows for its isolation from application programs with the goal of maintaining the integrity and the prevention of the policy from outside tampering (col.1, lines 16-30). The method includes requesting different security services managing a resource access policy, inquiring as to resource access decision, or for the subject registry (col.1, lines 37-43). Benantar discusses object oriented program include a system authorization policy object (SAP), SAO, and a system registration object (SAO) where the SAP object is used to retrieve and manipulated user capabilities that enlists the object that the

user is allowed access to, along with the corresponding access types or permission (col.2, lines 54-65). the user capability enlists the objects to which the user is allowed access along with the type of access that corresponds to the method the user can execute (col.5, lines 17-25). This includes management of subject capability for environment is capability based form based for authorization. Benantar discloses the user's capability enlists the object to which the user allowed access along with the type of access that corresponds to the methods the user can execute (col5, lines 10-28). Thus, Benantar obviously suggests the claimed enlistment object to enlist participants in the transaction.

Therefore it would have been obvious for a person of ordinary skills in the art to combine the teaching of transaction manager that includes kernel objects of Harman with enlistment object to enlist participants in the security system of Benantar because to improve security by maintaining the integrity and the prevention of the policy from outside tampering (Benantar - col.1, lines 16-30 and col5, lines 10-28).

As per claim 2: Cancelled

As per claim 3: see Harmon on col.11, lines 58-60 and Benantar on col.2, lines 58-60; discussing a system according to Claim 1, wherein the security descriptor comprises at least one access control entry (ACE), which includes a security identifier (SID) and rights corresponding to the SID.

As per claim 4: see Harmon on col.15, lines 1-2 and col.18, line 59 – col.19, line 11; discussing a system according to claim 1, wherein the security descriptor is applied to the transaction object, and the operation identified by the security descriptor includes at least one of: set information regarding the transaction object, enlist the transaction object in the transaction, render data

updates in connection with the transaction object durable, abort the operation on the transaction object, transmit data from the transaction object to another object, save the current point of the transaction at the transaction object, and transmit data regarding the transaction to another device.

As per claim 5: see Harmon on col.15, lines 1-2 and col.18, line 59 – col.19, line 11 and Benantar on col.1, lines 16-30 and col5, lines 10-28; discussing a system according to claim 1, wherein the security descriptor is applied to the resource manager object, and the operation identified by the security descriptor includes at least one of: retrieve information regarding the resource manager object, set information regarding the resource manager object, determine the state of a transaction at a moment of transaction failure, enlist the resource manager object in a transaction, register the resource manager object in the transaction, receive notification upon resolution of a transaction at the resource manager object, and set resource data in accordance with the transaction resolution.

As per claim 6: see Benantar on col.1, lines 16-30 and col5, lines 10-28**;** discussing a system according to claim 1, wherein the security descriptor is applied to the enlistment object, and the operation identified by the security descriptor includes at least one of: get information regarding the enlistment object, set information regarding the enlistment object, determine a state of enlistments at a moment of transaction failure obtain and reference an enlistment key, rollback the transaction and to respond to notifications, and perform operations a superior transaction manager would perform.

As per claim 7:

Harman discloses a method of implementing a kernel-level transaction, comprising:

attaching a security descriptor to at least one of plurality of kernel objects utilized in a transaction; and (col.14, lines 20-32 and col.15, lines 18-35; *modules being called or loaded by the kernel are given as kernel objects*)

performing an operation for a transaction on the at least one kernel object (col.14, lines 13-17 and col.18, lines 20-33) in accordance with the rights accorded by the security descriptor attached to the at least one kernel object, wherein the security descriptor includes identification for at least one user (col.13, lines 1-26), an operation that is able to be performed on the at least one kernel object to which the security descriptor is attached (col.18, line 59 – col.19, line 11), and a right indicating that the identified user is permitted or prohibited to perform the operation (col.20, lines 29-63), and further wherein the at least one kernel object comprises a transaction object (col.14, lines 42-50 and 58-67 and col.15, lines 36-40; *transaction module is given as security request and/or monitor associated with the application or service module*), a resource manager object (col.14, lines 30-42 and 51-52 and col.15, lines 55-67; *a resource object given as component, i.e. interface, controller, device server (col.17, lines 33-52)*) and/or an *[enlistment object].*

Although, Harman includes transaction object to represent a transaction which is a service module/application to plural kernel objects but does not go into details of an enlistment object to enlist participants.

Benantar's invention improves security in objected oriented system where the security system is a point of control for the security information and allows for its isolation from application programs with the goal of maintaining the integrity and the prevention of the policy from outside tampering (col.1, lines 16-30). The method includes requesting different security services managing a resource access policy, inquiring as to resource access decision, or for the

subject registry (col.1, lines 37-43). Benantar discusses object oriented program include a system authorization policy object (SAP), SAO, and a system registration object (SAO) where the SAP object is used to retrieve and manipulated user capabilities that enlists the object that the user is allowed access to, along with the corresponding access types or permission (col.2, lines 54-65). the user capability enlists the objects to which the user is allowed access along with the type of access that corresponds to the method the user can execute (col.5, lines 17-25). This includes management of subject capability for environment is capability based form based for authorization. Benantar discloses the user's capability enlists the object to which the user allowed access along with the type of access that corresponds to the methods the user can execute (col5, lines 10-28). Thus, Benantar obviously suggests the claimed enlistment object to enlist participants in the transaction.

Therefore it would have been obvious for a person of ordinary skills in the art to combine the teaching of transaction manager that includes kernel objects of Harman with enlistment object to enlist participants in the security system of Benantar because to improve security by maintaining the integrity and the prevention of the policy from outside tampering (Benantar - col.1, lines 16-30 and col5, lines 10-28).

As per claims 8-11: cancelled

As per claim 12: see Harmon on col.16, lines 20-46 and col.18, line 59 – col.19, line 11 and Benantar on col.1, lines 16-30 and col5, lines 10-28; discussing a method according to claim 7, wherein the operation identified by the security descriptor attached to the transaction object includes at least one of: set information regarding the transaction object, enlist the transaction object in the transaction, render data updates in connection with the transaction object durable,

abort the operation on the transaction object, transmit data from the transaction object to another object, save the current point of the transaction at the transaction object, and transmit data regarding the transaction to another device.

As per claim 13: see Harmon on col.16, lines 20-46 and col.18, line 59 – col.19, line 11 and Benantar on col.1, lines 16-30 and col5, lines 10-28; discussing a method according to claim 7, wherein the operation identified by the security descriptor attached to the resource manager object includes at least one of: retrieve information regarding the resource manager object, set information regarding the resource manager object, determine the state of a transaction at a moment of transaction failure, object, and enlist the resource manager object in a transaction, register the resource manager object in the transaction, receive notification upon resolution of a transaction at the resource manager set resource data in accordance with the transaction resolution.

As per claim 14: Benantar on col.1, lines 16-30 and col5, lines 10-28; discussing a method according to claim 7, wherein the operation identified by the security descriptor includes at least one of: get information regarding the enlistment object, set information regarding the enlistment object, determine a state of enlistments at a moment of transaction failure, obtain and reference an enlistment key, rollback the transaction and to respond to notifications, and perform operations a superior transaction manager would perform.

As per claim 15:

Harman discloses a computer-readable medium having stored thereon an object attached to a kernel object, the object comprising:

a first data entry identifying at least one user; (col.13, lines 1-26)

a second data entry identifying an operation (col.14, lines 13-17 and col.18, lines 20-33) capable of being performed on the kernel object by the user identified by the first data entry (col.18, line 59 – col.19, line 11), wherein the kernel object (col.14, lines 20-32 and col.15, lines 18-35; *modules being called or loaded by the kernel are given as kernel objects*) comprises a transaction object (col.14, lines 42-50 and 58-67 and col.15, lines 36-40; *transaction module is given as security request and/or monitor associated with the application or service module*), a resource manager object (col.14, lines 30-42 and 51-52 and col.15, lines 55-67; *a resource object given as component, i.e. interface, controller, device server (col.17, lines 33-52)*) and/or *[an enlistment object];* and

a third data entry indicating a right for the user identified by the first data entry to perform the operation identified by the second data entry; (col.20, lines 29-63)

wherein the object attached to the kernel object is a security descriptor. (col.14, lines 24-28 and col.17, lines 1-3)

Although, Harman includes transaction object to represent a transaction which is a service module/application to plural kernel objects but does not go into details of an enlistment object to enlist participants.

Benantar's invention improves security in objected oriented system where the security system is a point of control for the security information and allows for its isolation from application programs with the goal of maintaining the integrity and the prevention of the policy from outside tampering (col.1, lines 16-30). The method includes requesting different security services managing a resource access policy, inquiring as to resource access decision, or for the subject registry (col.1, lines 37-43). Benantar discusses object oriented program include a

system authorization policy object (SAP), SAO, and a system registration object (SAO) where the SAP object is used to retrieve and manipulated user capabilities that enlists the object that the user is allowed access to, along with the corresponding access types or permission (col.2, lines 54-65). the user capability enlists the objects to which the user is allowed access along with the type of access that corresponds to the method the user can execute (col.5, lines 17-25). This includes management of subject capability for environment is capability based form based for authorization. Benantar discloses the user's capability enlists the object to which the user allowed access along with the type of access that corresponds to the methods the user can execute (col5, lines 10-28). Thus, Benantar obviously suggests the claimed enlistment object to enlist participants in the transaction.

Therefore it would have been obvious for a person of ordinary skills in the art to combine the teaching of transaction manager that includes kernel objects of Harman with enlistment object to enlist participants in the security system of Benantar because to improve security by maintaining the integrity and the prevention of the policy from outside tampering (Benantar - col.1, lines 16-30 and col5, lines 10-28).

As per claim 16: see Harmon on col.16, lines 20-46 and col.18, line 59 – col.19, line 11 and Benantar on col.1, lines 16-30 and col5, lines 10-28; discussing a computer-readable medium according to Claim 15, wherein the kernel object is a transaction object, and the identified operation includes at least one of: set information regarding the transaction object, enlist the transaction object in the transaction, render data updates in connection with the transaction object durable, abort the operation on the transaction object, transmit data from the transaction object to another object, save the current point of the transaction at the transaction object, and transmit

data regarding the transaction to another device.

As per claim 17: see Harmon on col.16, lines 20-46 and col.18, line 59 – col.19, line 11 and Benantar on col.1, lines 16-30 and col5, lines 10-28; discussing a computer-readable medium according to Claim 15, wherein the kernel object is a resource manager object, and the identified operation includes at least one of: retrieve information regarding the resource manager object, set information regarding the resource manager object, determine the state of a transaction at a moment of transaction failure, enlist the resource manager object in a transaction, register the resource manager object in the transaction, receive notification upon resolution of a transaction at the resource manager object, and set resource data in accordance with the transaction resolution.

As per claim 18: see Harmon on col.16, lines 20-46 and col.18, line 59 – col.19, line 11 and Benantar on col.1, lines 16-30 and col5, lines 10-28; discussing a computer-readable medium according to Claim 15, wherein the kernel object is an enlistment object, and the identified operation includes at least one of: get information regarding the enlistment object, set information regarding the enlistment object, determine a state of enlistments at a moment of transaction failure, obtain and reference an enlistment key, rollback the transaction and to respond to notifications, and perform operations a superior transaction manager would perform.

As per claim 19:

Harman discloses a transaction method, comprising:

implementing a transaction among kernel objects; (col.14, lines 20-32 and col.15, lines 18-35; *modules being called or loaded by the kernel are given as kernel objects*)

securing the transaction utilizing an operating system security model that applies a security descriptor to at least one of the kernel objects participating in the transaction; (col.18, line 59 – col.19, line 11)

wherein the security descriptor includes identification for at least one user (col.13, lines 1-26), an operation to be performed on the at least one kernel object to which the security descriptor is attached (col.14, lines 13-17 and col.18, lines 20-33), and a right indicating that the identified user is permitted or prohibited to perform the operation (col.20, lines 29-63) and each of the kernel objects comprise a transaction object (col.14, lines 42-50 and 58-67 and col.15, lines 36-40; *transaction module is given as security request and/or monitor associated with the application or service module*), a resource manager object (col.14, lines 30-42 and 51-52 and col.15, lines 55-67; *a resource object given as component, i.e. interface, controller, device server (col.17, lines 33-52)*) and/or *[an enlistment object].*

Although, Harman includes transaction object to represent a transaction which is a service module/application to plural kernel objects but does not go into details of an enlistment object to enlist participants.

Benantar's invention improves security in objected oriented system where the security system is a point of control for the security information and allows for its isolation from application programs with the goal of maintaining the integrity and the prevention of the policy from outside tampering (col.1, lines 16-30). The method includes requesting different security services managing a resource access policy, inquiring as to resource access decision, or for the subject registry (col.1, lines 37-43). Benantar discusses object oriented program include a system authorization policy object (SAP), SAO, and a system registration object (SAO) where

the SAP object is used to retrieve and manipulated user capabilities that enlists the object that the user is allowed access to, along with the corresponding access types or permission (col.2, lines 54-65). the user capability enlists the objects to which the user is allowed access along with the type of access that corresponds to the method the user can execute (col.5, lines 17-25). This includes management of subject capability for environment is capability based form based for authorization. Benantar discloses the user's capability enlists the object to which the user allowed access along with the type of access that corresponds to the methods the user can execute (col5, lines 10-28). Thus, Benantar obviously suggests the claimed enlistment object to enlist participants in the transaction.

Therefore it would have been obvious for a person of ordinary skills in the art to combine the teaching of transaction manager that includes kernel objects of Harman with enlistment object to enlist participants in the security system of Benantar because to improve security by maintaining the integrity and the prevention of the policy from outside tampering (Benantar - col.1, lines 16-30 and col5, lines 10-28).

As per claim 20: Cancelled.

As per claim 21:

Harman discloses a method of implementing a transaction, comprising:

attaching a security descriptor to at least one of a plural of objects (col.14, lines 20-32 and col.15, lines 18-35; *modules being called or loaded by the kernel are given as kernel objects*) utilized in a transaction, wherein the security descriptor includes identification for at least one user (col.13, lines 1-26), an operation (col.14, lines 13-17 and col.18, lines 20-33) to be performed on the at least one kernel object to which the security descriptor is attached, and a

right indicating that the identified user is permitted or prohibited to perform the operation (col.18, line 59 – col.19, line 11) and each of the kernel objects comprise a transaction object (col.14, lines 42-50 and 58-67 and col.15, lines 36-40; *transaction module is given as security request and/or monitor associated with the application or service module*), a resource manager object (col.14, lines 30-42 and 51-52 and col.15, lines 55-67; *a resource object given as component, i.e. interface, controller, device server (col.17, lines 33-52)*) and/or *[an enlistment object.]*

performing an operation for a transaction on the at least one object in accordance with the rights accorded by the security descriptor attached to the at least one object. (col.20, lines 29-63)

Although, Harman includes transaction object to represent a transaction which is a service module/application to plural kernel objects but does not go into details of an enlistment object to enlist participants.

Benantar's invention improves security in objected oriented system where the security system is a point of control for the security information and allows for its isolation from application programs with the goal of maintaining the integrity and the prevention of the policy from outside tampering (col.1, lines 16-30). The method includes requesting different security services managing a resource access policy, inquiring as to resource access decision, or for the subject registry (col.1, lines 37-43). Benantar discusses object oriented program include a system authorization policy object (SAP), SAO, and a system registration object (SAO) where the SAP object is used to retrieve and manipulated user capabilities that enlists the object that the user is allowed access to, along with the corresponding access types or permission (col.2, lines 54-65). the user capability enlists the objects to which the user is allowed access along with the type of access that corresponds to the method the user can execute (col.5, lines 17-25). This

includes management of subject capability for environment is capability based form based for authorization. Benantar discloses the user's capability enlists the object to which the user allowed access along with the type of access that corresponds to the methods the user can execute (col5, lines 10-28). Thus, Benantar obviously suggests the claimed enlistment object to enlist participants in the transaction.

Therefore it would have been obvious for a person of ordinary skills in the art to combine the teaching of transaction manager that includes kernel objects of Harman with enlistment object to enlist participants in the security system of Benantar because to improve security by maintaining the integrity and the prevention of the policy from outside tampering (Benantar - col.1, lines 16-30 and col5, lines 10-28).

As per claim 22-25: see Harmon on col.16, lines 20-46 and col.18, line 59 – col.19, line 11 and Benantar on col.1, lines 16-30 and col5, lines 10-28; discussing a method according to Claim 21, wherein the security descriptor includes identification for at least one user, an operation to be performed on the at least one object to which the security descriptor is attached, and a right indicating that the identified user is permitted or prohibited to perform the operation.

As per claim 26: see Harmon on col.16, lines 20-46 and col.18, line 59 – col.19, line 11 and Benantar on col.1, lines 16-30 and col5, lines 10-28; discussing a method according to claim 21, wherein the operation identified by the security descriptor attached to the transaction object includes at least one of: set information regarding the transaction object, enlist the transaction object in the transaction, render data updates in connection with the transaction object durable, abort the operation on the transaction object, transmit data from the transaction object to another object, save the current point of the transaction at the transaction object, and transmit data

regarding the transaction to another device.

As per claim 27: see Harmon on col.16, lines 20-46 and col.18, line 59 – col.19, line 11 and Benantar on col.1, lines 16-30 and col5, lines 10-28; discussing a method according to claim 21, wherein the operation identified by the security descriptor attached to the resource manager object includes at least one of: retrieve information regarding the resource manager object, set information regarding the resource manager object, determine the state of a transaction at a moment of transaction failure, enlist the resource manager object in a transaction, register the resource manager object in the transaction, receive notification upon resolution of a transaction at the resource manager object, and set resource data in accordance with the transaction resolution.

As per claim 28: see Harmon on col.16, lines 20-46 and col.18, line 59 – col.19, line 11 and Benantar on col.1, lines 16-30 and col5, lines 10-28; discussing a method according to claim 21, wherein the operation identified by the security descriptor includes at least one of: get information regarding the enlistment object, set information regarding the enlistment object, determine a state of enlistments at a moment of transaction failure, obtain and reference an enlistment key, rollback the transaction and to respond to notifications, and perform operations a superior transaction manager would perform.

As per claim 29:

Harman discloses a kernel-level transaction system, comprising:

a memory; (col.11, lines 4-13 and col.12, lines 48-50)

one or more processors operatively coupled to the memory; (col.12, lines 32-60)

means for implementing a transaction among kernel objects (col.14, lines 20-32 and col.15, lines 18-35; *modules being called or loaded by the kernel are given as kernel objects*), wherein the kernel objects include a transaction object to represent a transaction (col.14, lines 42-50 and 58-67 and col.15, lines 36-40; *transaction module is given as security request and/or monitor associated with the application or service module*), a resource manager object to represent a resource participating in the transaction (col.14, lines 30-42 and 51-52 and col.15, lines 55-67; *a resource object given as component, i.e. interface, controller, device server (col.17, lines 33-52)*), and *[an enlistment object to enlist participants in the transaction]*, wherein the transaction is performed at the kernel level; and (col.14, lines 24-28 and col.17, lines 1-3)

means for securing the transaction by applying a security descriptor to at least one of the kernel objects, wherein the security descriptor identifies at least one user (col.13, lines 1-26), an operation to be performed on the kernel object to which the security descriptor is applied (col.18, line 59 – col.19, line 11), and a right indicating that the identified user is permitted or prohibited to perform the operation. (col.20, lines 29-63)

Although, Harman includes transaction object to represent a transaction which is a service module/application to plural kernel objects but does not go into details of an enlistment object to enlist participants.

Benantar's invention improves security in objected oriented system where the security system is a point of control for the security information and allows for its isolation from application programs with the goal of maintaining the integrity and the prevention of the policy from outside tampering (col.1, lines 16-30). The method includes requesting different security services managing a resource access policy, inquiring as to resource access decision, or for the

subject registry (col.1, lines 37-43). Benantar discusses object oriented program include a system authorization policy object (SAP), SAO, and a system registration object (SAO) where the SAP object is used to retrieve and manipulated user capabilities that enlists the object that the user is allowed access to, along with the corresponding access types or permission (col.2, lines 54-65). the user capability enlists the objects to which the user is allowed access along with the type of access that corresponds to the method the user can execute (col.5, lines 17-25). This includes management of subject capability for environment is capability based form based for authorization. Benantar discloses the user's capability enlists the object to which the user allowed access along with the type of access that corresponds to the methods the user can execute (col5, lines 10-28). Thus, Benantar obviously suggests the claimed enlistment object to enlist participants in the transaction.

Therefore it would have been obvious for a person of ordinary skills in the art to combine the teaching of transaction manager that includes kernel objects of Harman with enlistment object to enlist participants in the security system of Benantar because to improve security by maintaining the integrity and the prevention of the policy from outside tampering (Benantar - col.1, lines 16-30 and col5, lines 10-28).

As per claim 30: cancelled.

As per claim 31: see Harmon on col.16, lines 20-46 and col.18, line 59 – col.19, line 11 and Benantar on col.1, lines 16-30 and col5, lines 10-28; discussing a system according to claim 29, wherein the security descriptor is applied to the transaction object, and the operation identified by the security descriptor includes at least one of: set information regarding the transaction object, enlist the transaction object in the transaction, render data updates in connection with the

transaction object durable, abort the operation on the transaction object, transmit data from the transaction object to another object, save the current point of the transaction at the transaction object, and transmit data regarding the transaction to another device.

As per claim 32: see Harmon on col.16, lines 20-46 and col.18, line 59 – col.19, line 11 and Benantar on col.1, lines 16-30 and col5, lines 10-28; discussing a system according to claim 29, wherein the security descriptor is applied to the resource manager object, and the operation identified by the security descriptor includes at least one of: retrieve information regarding the resource manager object, set information regarding the resource manager object, determine the state of a transaction at a moment of transaction failure, enlist the resource manager object in a transaction, register the resource manager object in the transaction, receive notification upon resolution of a transaction at the resource manager object, and set resource data in accordance with the transaction resolution.

As per claim 33: see Benantar on col.1, lines 16-30 and col5, lines 10-28; discussing a system according to claim 29, wherein the security descriptor is applied to the enlistment object, and the operation identified by the security descriptor includes at least one of: get information regarding the enlistment object, set information regarding the enlistment object, and determine a state of enlistments at a moment of transaction failure.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Leynna T. Truvan whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/L. T. T./
Examiner, Art Unit 2135
/KimYen Vu/
Supervisory Patent Examiner, Art Unit 2135